Cyolo

The 'Last Mile' of Application Security: Extending Your Secure Access Service Edge (SASE)

Organizations today must adapt quickly in order to survive. This became clearer than ever when the COVID-19 pandemic forced a huge portion of the workforce out of the office and into remote work. It was in this environment that the Secure Access Service Edge (SASE, pronounced sassy) was born. SASE is the meeting point between a wide area network (WAN) and cloud-delivered security services such as Secure Web Gateways (SWGs), Cloud Firewalls, and Zero Trust Network Access (ZTNA). Combined, these services bring needed flexibility to remote workers and security controls to the business.

For many organizations, SASE results in better business adaptivity, increased performance, improved threat detection and mitigation, and cost savings. It is clear why companies are deploying SASE solutions. But despite these real benefits, **SASE comes with two major drawbacks that leave a dangerous gap in the "last mile" of application security for most companies.**

1. Like most cloud-delivered solutions, SASE secures and protects cloud resources well. However, many enterprises still utilize legacy systems such as mainframes and on-premises tools, such as Enterprise Resource Planning (ERP), which remain unprotected by SASE controls.

2. Like more traditional perimeter-focused security tools, SASE focuses on the network. This is an outdated approach that does not account for today's new security reality, in which identity is the primary security perimeter. Without the ability to weave an identity fabric and make access decisions based on a single, auditable, digital identity, SASE solutions are limited from the start.

Organizations looking to protect their last mile of vulnerability must solve these two issues.

> *While modern SASE solutions can protect significant portions of an organization's attack surface, their cloud-based approach leaves gaps that bad actors can exploit.*

Gartner predicts that **40%** of enterprises will have defined SASE strategies by 2026.

Without a single place to merge all of the organization's various identity providers across on-premises data centers and the cloud, SASE becomes nothing more than another network for users to transit. Meeting compliance requirements and passing audits will also be tricky without the ability to trace application access back to a single identity. Indeed, those utilizing on-premises legacy applications or overseeing critical infrastructure, such as Operational Technology (OT) networks, must recognize that SASE solutions cannot protect these resources without violating compliance mandates.

SASE solutions have their greatest success protecting modern, cloud-native resources. However, they struggle to bring the same level of security and connectivity into the organization's secure boundaries and legacy applications. To achieve full protection for your last mile of applications, augment your SASE tool with a zero-trust access and connectivity solution that covers everything, everywhere, for everyone.

To extend security controls to legacy, on-premises, and homegrown applications, Cyolo is the only solution. Cyolo brings modern authentication and identity-based connectivity to legacy applications and OT systems by sitting in front of these applications and brokering the connection securely and quickly. Cyolo also layers multifactor-authentication (MFA) with single sign-on (SSO) to ensure that only verified users can connect.

When combined with a SASE platform, Cyolo becomes the single source of truth for digital identity and access policies. With Cyolo, organizations can streamline all existing identity providers, retrofit legacy resources with modern authentication and connectivity, and create a single policy enforcement point across all users, applications, and devices.

'LAST MILE' APPLICATIONS

- Leave systems unprotected
- Create vulnerability
- Compromise security controls
- Allow for cyberattacks
- Cause security incidents

> *To achieve full protection for your last mile of applications, augment your SASE tool with a zero-trust access and connectivity solution that covers everything, everywhere, for everyone.*